*The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.*

**DATE ISSUED:**

04/08/2014

**SUBJECT:**

Vulnerability in Microsoft Publisher Could Allow Remote Code Execution (MS14-020)

**EXECUTIVE SUMMARY:**

Microsoft Publisher's vulnerability could allow remote code execution if a user opens a specially crafted file in an affected version of Microsoft Publisher. Microsoft Publisher is an entry-level desktop publishing application from Microsoft, differing from Microsoft Word in that the emphasis is placed on page layout and design rather than text composition and proofing. Customers whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user.

**THREAT INTELLIGENCE:**

At this time these vulnerabilities are not publicly disclosed and there is no known proof-of-concept code available.

**SYSTEMS AFFECTED:**

- Microsoft Office 2003 Service Pack 3
- Microsoft Office 2007 Service Pack 3

**RISK:**

**Government:**

- Large and medium government entities: High

- Small government entities: High

**Businesses:**

- Large and medium business entities: High
- Small business entities: High

**Home users: High**

**TECHNICAL SUMMARY:**

A remote code execution vulnerability exists in the way that affected versions of Microsoft Publisher parses specially crafted files. An attacker who successfully exploited this vulnerability could run arbitrary code as the current user. If the current user is logged on with administrative user rights, an attacker could take complete control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

**RECOMMENDATIONS:**

The following actions should be taken:

- Install the updates provided by Microsoft immediately after appropriate testing.
- Remind users not to visit untrusted websites or follow links provided by unknown or untrusted sources.
- Do not open email attachments from unknown or untrusted sources.

**REFERENCES:**

**Microsoft:**

https://technet.microsoft.com/en-us/security/bulletin/ms14-020

**CVE:**

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1759